REMARKS

The rejections presented in the Office Action dated October 5, 2004 have been considered. Claims 1-16 remain pending in the application. Reconsideration and allowance of the application are respectfully requested.

The Office Action fails to establish that claims 1 - 16 are unpatentable under 35 USC §103(a) over "Moore" (US patent number 6,678,700 to Moore et al.) in view of "Moskowitz" (US patent publication number 20020071556A1 to Moskowitz et al.) and further in view of "Brundrett" (US patent number 6,249,866 to Brundrett et al.). The rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references, fails to provide a proper motivation for modifying the teachings of Moore with teachings of Moskowitz, fails to provide a proper motivation for modifying the teachings of the Moore-Moskowitz combination with teachings of Brundrett, and fails to show that the combination could be made with a reasonable likelihood of success.

As to claims 1, 13, and 14, the Office Action fails to show that the combination suggests the various limitations. For example, Moskowitz is not shown to suggest generating an encryption key at the metadata server and at the storage server and storing the key in the security object. The cited paragraph 0023 of Moskowitz discusses breaking an encryption key into partial keys. There is no suggestion of generating a key by a metadata server and a storage server, nor is there any apparent suggestion of storing the key in the security object. Furthermore, the cited teachings of Moore neither teach nor suggest that a metadata server and storage server generate the key.

Brundrett is not shown to suggest the limitations of and related to storing the key in the security object, encrypting a list that identifies a set of blocks in the opened file, and adding the encrypted list to the security object. The Office Action cites Brundrett's teaching of an "encrypting file system driver" communicating with an "EFS service by passing it the file metadata, including the data decryption and data recovery fields" as teaching these limitations. However, there is no cited or readily apparent suggestion that Brundrett suggests encrypting a list that identifies a set of blocks in the opened file, nor any apparent suggestion of adding the encrypted list to the security object. Since Brundrett does not appear to use a distributed file system interface along with the claimed meta-data server and block storage server, Brundrett would have no apparent need to encrypt the list of blocks for transmission back to a distributed file system interface. Furthermore, those skilled in the art will recognize

the distinction between encrypting a list that identifies blocks in a file versus encrypting the file data.

No teaching has been cited as suggesting the transmitting of the claimed security object to a distributed file system interface.

In addition to failing to show a suggestion of the various limitations of claims 1, 13, and 14, the Office Action also fails to provide proper motivations for combining Moskowitz with Moore and for combining Brundrett with the Moore-Moskowitz combination.

The alleged motivation for modifying Moore with Moskowitz is conclusory, based on hindsight and therefore, improper. The alleged motivation is that "it would have been obvious ... to use partial keys created at different servers as in the system of Moskowitz and adding the keys to the data portion of the object in the system of Moore, thus creating a security object ... because sharing the secret between more devices increase the amount of security since both values are required fore [sic] decrypting the message." This alleged motivation merely states a function of partial keys. No clear and particular evidence is provided that would motivate one to modify Moore's system. Moore's system is presumably adequate for its intended purpose, and no evidence is provided to indicate any deficiencies in Moore's system. Thus, the alleged motivation is merely a reconstruction of the claim limitations based on hindsight.

The alleged motivation for modifying the Moore-Moskowitz combination with Brundrett is also conclusory, based on hindsight and therefore, improper. The alleged motivation is "that it would have been obvious ... to encrypt the file as in Brundrett and adding the encrypted information to the data portion of the object in the system of Moore ... because encryption secures the information." This alleged motivation simply states the function of encryption. No evidence is provided to suggest a desirability of modifying the Moore-Moskowitz combination. Thus, the alleged motivation is merely a reconstruction of the claim limitations based on hindsight.

As to claim 2, the Office Action fails to show that the limitations are suggested by the Moore-Moskowitz-Brundrett combination, and the alleged motivation is improper. As indicated above, the Office Action does not show any element in the Moore-Moskowitz-Brundrett combination as corresponding to a distributed file system interface. Therefore, there is no apparent correspondence of transmitting a file access request and the claimed security object from the distributed file system interface to a storage server. Furthermore, the Office Action cites Brundrett's decrypting of text. However, the cited col. 17 of Brundrett

teaches that the file data is decrypted. There is no apparent correspondence between the claimed decrypting of the block list (which identifies a set of blocks in the file) and Brundrett's decrypting of file data. Therefore, the limitations of claim 2 are not shown to be suggested by the Moore-Moskowitz-Brundrett combination. Also, the alleged motivation for modifying the Moore-Moskowitz combination with the cited teachings of Brundrett is improper as being conclusory and based on hindsight. That is, the alleged motivation simply states a function of decryption without providing any evidence to motivate the combination.

Claims 3, 4, 8, 9 and 16 depend from the claims discussed above and are patentable over the Moore-Moskowitz-Brundrett combination for at least the reasons set forth above.

As to claims 5 and 10, the Office Action does not show that Moore teaches or suggests the limitations of removing the encrypted block list of the first file from the security object. Moore's FIG. 10, element 75 is cited as suggesting this limitation. However, there is no apparent suggestion that anything is removed from a security object, much less an encrypted block list. Thus, claims 5 and 10 are not shown to be unpatentable over the Moore-Moskowitz-Brundrett combination.

In claims 6 and 11, the security object minus the encrypted block list is returned to the distributed file system interface. The cited FIG. 16B of Moore discusses synchronizing a copy of a container having an updated data object between a physical resource and other copies of the container on a network. There is no apparent transmission of any security object minus a block list as claimed.

Claims 7 and 12 depend from claims 6 and 11, respectively. Thus, claims 7 and 12 are patentable over the Moore-Moskowitz-Brundrett combination for at least the reasons set forth above.

Claim 15 includes limitations of the storage server being configured to decrypt the encrypted block list in response to the file access request and provide access to the selected data in accordance with the operation code upon successful decryption of the block list. As explained above, Brundrett suggests decrypting file data, not decrypting a block list. Therefore, the Office Action fails to show that claim 15 is unpatentable over the Moore-Moskowitz-Brundrett combination.

The rejection of claims 1-16 over the Moore-Moskowitz-Brundrett combination should be withdrawn because the Office Action fails to show all the limitations are suggested by the combination, fails to provide a proper motivation for combining the references, and fails to show that the combination could be made with a reasonable likelihood of success.

Withdrawal of the rejections and reconsideration of the claims are respectfully requested in view of the remarks set forth above.

Respectfully submitted,

CRAWFORD MAUNU PLLC
1270 Northland Drive, Suite 390
Saint Paul, MN 55120
(651) 686-6633

By: 
Name: LeRoy D. Maunu
Reg. No.: 35,274